



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/670,604	09/26/2003	Tetsuro Motoyama	240204US28	1499
22850	7590	10/05/2007		
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER SIKRI, ANISH	
			ART UNIT 2143	PAPER NUMBER
			NOTIFICATION DATE 10/05/2007	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

8

<b>Office Action Summary</b>	<b>Application No.</b> 10/670,604	<b>Applicant(s)</b> MOTOYAMA, TETSURO	
	<b>Examiner</b> Anish Sikri	<b>Art Unit</b> 2143	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 01 August 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 August 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>See Continuation Sheet</u> . | 6) <input type="checkbox"/> Other: _____  |

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :12/29/03, 04/27/04, 11/09/04, 3/18/05, 5/24/05, 12/21/05, 12/05/06, 09/07/07.

**DETAILED ACTION**

***Information Disclosure Statement***

The information disclosure statement submitted on 12/29/03, 04/27/04, 11/09/04, 3/18/05, 5/24/05, 12/21/05, 12/05/06, 09/07/2007 has been considered by the Examiner and made of record in the application file.

***Claim Rejections - 35 USC § 102***

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Ramberg et al (US Pub 20030014505 A1).

Consider **Claim 1**, Ramberg et al clearly discloses a method of storing information configured to be used for a plurality of communication protocols to access a monitored device by a monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]) among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), comprising: retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device (Ramberg et al, [0038], Fig 3, [0046], [0047], [0049], [0052]) it clearly shows that the management information base contains the information about the sets of objects, and provides information about each object – including its structure and relationship with other objects. It also shows on the use of a system management unit, which aids in management of devices;

Storing by the monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]), in a second memory, the information for accessing the monitored device

Art Unit: 2143

retrieved from the first memory (Ramberg et al, [0038]-[0039]) (There is also a MIB on the device, which tells SNMP agents information about the devices;

Selecting by the monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]) a communication protocol among the plurality of communication protocols (Ramberg et al, [0024], [0099]); the monitored device being configured to process two or more of the plurality of communication protocols;

and directly accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory by the monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]). It clearly shows on how monitoring systems employ plurality of communication protocols to be used to monitor devices in the network. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 2**, and as applied to claim 1 above, Ramberg et al clearly discloses the method wherein the retrieving step comprises: accessing a memory external to a monitoring computer to obtain the information for accessing the monitored device (Ramberg et al, [0025], [0038], [0039], Fig 3, [0046], [0047], [0049], [0052]). It clearly shows on the use of remote computing system to monitor devices in the network.

Art Unit: 2143

The management information base is also tied with the application which monitors the devices on the network via SNMP (Ramberg et al, [0039]).

Consider **Claim 3**, and as applied to claim 1 above, Ramberg et al clearly discloses the method, wherein the selecting step comprises: selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols, which can be used for monitoring devices, comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 4**, and as applied to claim 1 above, Ramberg et al clearly discloses the method, wherein the retrieving step comprises: retrieving, from the first memory, at least one of a username and a password for accessing the monitored device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 5**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: retrieving, from the first memory, at least one of a community name and a password for accessing the monitored device

Art Unit: 2143

using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 6**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: retrieving, from the first memory, an IP address of the monitored device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 7**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the second memory comprises a vector of parameter name and parameter value pairs for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can be used with other programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 8**, and as applied to claim 1 above, Ramberg et al clearly discloses the storing step comprises: storing the information for accessing the monitored device in a device software object associated with the monitored device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.



Consider **Claim 9**, and as applied to claim 8 above, Ramberg et al clearly discloses wherein the device software object is stored in a random-access memory unit of the monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function (Ramberg et al, [0051]).

Consider **Claim 10**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the retrieving step comprises: accessing the first memory using virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Interface, as it uses XML. And the XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 11**, and as applied to claim 1 above, Ramberg et al clearly discloses wherein the accessing step comprises: transmitting to the monitored device, information stored in the second memory necessary to access the monitored device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041], Fig 3, [0046], [0047], [0049], [0052]). It clearly shows on the usage of memory on the

Art Unit: 2143

system(s) when monitoring functionality is carried out when accessing the device via SNMP.

Consider **Claim 12**, and as applied to claim 11 above, Ramberg et al clearly discloses wherein the accessing step comprises: receiving, by the monitored device, the transmitted information; and processing, by the monitored device, the received information (Ramberg et al, [0038]-[0039], [0040]-[0041], Fig 3, [0046], [0047], [0049], [0052]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

Consider **Claim 13**, Ramberg et al clearly discloses a system of storing information configured to be used for a plurality of communication protocols to access a monitored device by a monitoring device (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]) among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), comprising: means of retrieving, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]), said means for retrieving being disposed in the monitoring computer; (It clearly shows that the management information base contains the information about the sets of objects, and provides information about each object – including its structure and relationship with other objects); It also shows on the use of a system management unit, which aids in management of devices

means of storing, in a second memory, the information for accessing the monitored device retrieved from the first memory, said means for storing being disposed in the monitoring computer; (Ramberg et al, Page 1, Fig 3, [0046], [0047], [0049], [0052]) (There is also a MIB on the device, which tells SNMP ages information about the devices) It also shows on the use of a system management unit, which aids in management of devices;

means for selecting a communication protocol among the plurality of communication protocols (Ramberg et al, Page 1, [0024], [0099]), said means for selecting being disposed in the monitoring computer, the monitored device being configured to process two or more of the plurality of communication protocols;

Art Unit: 2143

and means for accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory disposed in the monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]). It clearly shows on how monitoring systems employ plurality of communication protocols to be used to monitor devices in the network. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 14**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for accessing a memory external to a monitoring computer to obtain the information for accessing the monitored device (Ramberg et al, [0025], [0038], [0039]). It clearly shows on the use of remote computing system to monitor devices in the network. The management information base is also tied with the applications, which monitors the devices on the network via SNMP (Ramberg et al, [0039]).

Consider **Claim 15**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for selecting step comprises: means for selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols which can be used for monitoring devices comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate

Art Unit: 2143

information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 16**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, at least one of a username and a password for accessing the monitored device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 17**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, at least one of a community name and a password for accessing the monitored device using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 18**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: means for retrieving, from the first memory, an IP address of the monitored device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 19**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the second memory comprises a vector of parameter name and

Art Unit: 2143

parameter value pairs for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can be used with other programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 20**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for storing step comprises: means for storing the information for accessing the monitored device in a device software object associated with the device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.

Consider **Claim 21**, and as applied to claim 20 above, Ramberg et al clearly discloses wherein the device software object is stored in a random-access memory unit of the monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on a computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function properly (Ramberg et al, [0051]).

Consider **Claim 22**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for retrieving step comprises: accessing the first memory

using virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Interface, as it uses XML. And the XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 23**, and as applied to claim 13 above, Ramberg et al clearly discloses wherein the means for accessing step comprises: means for transmitting to the monitored device, information stored in the second memory necessary to access the monitored device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows on the usage of memory on the system(s) when monitoring functionality is carried out when accessing the device(s) via SNMP.

Consider **Claim 24**, and as applied to claim 23 above, Ramberg et al clearly discloses wherein the means for accessing step comprises: means for receiving, by the monitored device, the transmitted information; and means for processing, by the monitored device, the received information (Ramberg et al, [0038]-[0039], [0040]-[0041], Fig 3, [0046], [0047], [0049], [0052]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

Consider **Claim 25**, A computer readable storage medium encoded with instructions which when executed by a processing apparatus cause the processing apparatus to implement a method of storing information configured to be used for a plurality of communication protocols to access a monitored device (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]) by a monitoring computer among distinct devices communicatively coupled to a network (Ramberg et al, [0024]), the method comprising: Retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol (Ramberg et al, Page 1, [0024], [0099]) supported by the monitored device Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]);

Storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]);

Selecting by the monitoring computer a communication protocol among the plurality of communication protocols (Ramberg et al, Page 1, [0024], [0099]), the monitored device being configured to process two or more of the plurality of communication protocols (Ramberg et al, Page 1, [0024], [0099]); and

Accessing the monitored device (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]) using the selected communication protocol (Ramberg et al, Page 1, [0024], [0099]) and the information retrieved from the first memory and stored in the second memory by the monitoring computer (Ramberg et al, Fig 3, [0046], [0047], [0049],



[0052]). It also shows on the use of a system management unit, which aids in management of devices.

Consider **Claim 26**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the means for retrieving comprises: for accessing a memory external to a monitoring computer to obtain the information for accessing the monitored device (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]). It clearly shows on the use of remote computing system to monitor devices in the network. The management information base is also tied with the applications, which monitors the devices on the network via SNMP (Ramberg et al, [0039]). It also shows on the use of a system management unit, which aids in management of devices.

Consider **Claim 27**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium wherein the selecting step comprises: means for selecting a communication protocol among SNMP, HTTP, and FTP (Ramberg et al, [0024], [0099]). It clearly shows that few of the protocols, which can be used for monitoring devices, comprises of the protocols SNMP, HTTP and FTP. The monitoring systems translate information within the monitored devices into appropriate communication formats (Ramberg et al, [0024]).

Consider **Claim 28**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium for retrieving step comprises:

instructions for retrieving, from the first memory, at least one of a username and a password for accessing the device using FTP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use passwords on the devices in the network when accessing them for monitoring.

Consider **Claim 29**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium for retrieving step comprises: means for retrieving, from the first memory, at least one of a community name and a password for accessing the monitored device using SNMP (Ramberg et al, [0078], [0094], [0099]). It clearly shows on the use of SNMP along with passwords for monitoring devices in the network.

Consider **Claim 30**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium for retrieving step comprises: means for retrieving, from the first memory, an IP address of the monitored device (Ramberg et al, [0046]). It clearly shows that the devices in the network have an IP address.

Consider **Claim 31**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium comprises the second memory where a vector of parameter name and parameter value pairs for each of the plurality of communication protocols (Ramberg et al, [0055], [0056]). The SNMP subagents in Ramberg et al's invention uses routines as vectors, as they can used with other

programs (Ramberg et al, [0055]). The routines are stored separately as files, and are pointed to when being used (Ramberg et al, [0055]).

Consider **Claim 32**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein the readable storage medium for storing step comprises: means for storing the information for accessing the monitored device in a device software object associated with the monitored device (Ramberg et al, [0040], [0044]-[0045]). It clearly shows that device data is captured from the device and stored in a database.

Consider **Claim 33**, and as applied to claim 32 above, Ramberg et al clearly discloses wherein readable storage medium the device software object in random-access memory unit of the monitoring computer (Ramberg et al, [0051]). It clearly shows that during monitoring the application software is incorporating the use of system memory. The remote HTML browser which is the remote monitoring console runs on a computer, UNIX workstation, host computer etc. These systems have random-access memory unit to function properly (Ramberg et al, [0051]).

Consider **Claim 34**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein readable storage medium for retrieving step comprises: accessing the first memory using virtual functions associated with an abstract software class (Ramberg et al [0040]-[0041], [0047]). Ramberg et al clearly shows that the platform devices can be managed by the use of Dynamic User Interface, as it uses XML. And the

Art Unit: 2143

XML provides a data standard to encode the content, semantics, and schemata for communication. The Java system management can also be used (which contains classes) for communication with SNMP agents [0049].

Consider **Claim 35**, and as applied to claim 25 above, Ramberg et al clearly discloses wherein readable storage medium for accessing step comprises: instructions for transmitting to the monitored device, information stored in the second memory necessary to access the monitored device using the selected communication protocol (Ramberg et al, [0038]-[0039], [0040]-[0041]). It clearly shows on the usage of memory on the system(s) when monitoring functionality is carried out when accessing the device(s) via SNMP.

Consider **Claim 36**, and as applied to claim 35 above, Ramberg et al clearly discloses wherein the readable storage medium for accessing step comprises: means for receiving, by the monitored device, the transmitted information; and means for processing, by the monitored device, the received information (Ramberg et al, Fig 3, [0046], [0047], [0049], [0052]). It clearly shows that during monitoring, both the system monitor and the monitored devices transmit information to each other and vice-versa.

***Response to Arguments***

Applicant's arguments filed 8/1/07 have been fully considered but they are not persuasive.

In response to applicant's argument that 1, 13, and 25, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Applicant argues because of reliance of an argument that Ramberg et al does not disclose the method/unit described in claims 1, 13, and 25. Applicant states "remote computing system 120 does not directly access the monitored device (ADC Device 101 or 102). On the contrary, any query sent by the computer of Ramberg et al needs to be relayed through the SNMP master agent 220 before the query is sent to the ADC device 101 or 102. This is because the ADC device 101 or 102 only processes data in one communication protocol, and the SNMP master agent has to convert the format of the query into SNMP and the SNMP subagent has to convert the SNMP into the one communication protocol used by ADC device 101 or 102. Thus, the remote computer 120 does not directly access the monitored device (ADC device 101 or 102)".

Please refer to the reference cited by the Examiner (Ramberg et al, US Pub 20030014505 A1).

Further more, the reference Ramberg et al (US Pub 20030014505 A1) clearly shows on the use of a remote computing system, which monitors devices (Ramberg et al, [0046]-[0049]). It shows on the use of a system management support unit, which communicates with the remote computing system using sockets, TCP, UDP etc. It clearly shows that it can operate with multiple protocols.

Additional support can also be found with the use of a Management Information Base (MIB). The MIB communicates with the SNMP devices while providing information about each object, and operations allowed on the object. SNMP is the network management protocol of the Transmission Control/Internet Protocol. It clearly shows that the protocol being used is TCP/IP. It may also use UDP communication methods. As UDP is another protocol stack used in TCP/IP communication suite (Ramberg et al, [0037]-[0038]-[0039], [0043]).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

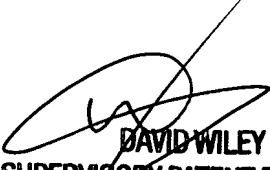
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anish Sikri whose telephone number is 571-270-1783. The examiner can normally be reached on 8am - 5pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on 571-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Anish Sikri  
a.s.

September 22, 2007

  
**DAVID WILEY**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**